Tripwire Version 1.0.0.0 for Solaris 2.5.1

PURPOSE:

Tripwire is an integrity checker. It will scan the files you tell it to scan in the Tripwire configuration file, and determine if they have been replaced, modified, or otherwise amended. This functionality is useful to detect unauthorized changes made by authorized users, and to determine what damage your system has sustained after an intrusion.

Example Application: Tripwire will identify any Trojan horses left behind by an intruder, provided the directory and/or file of the Trojan horse is included in the Tripwire configuration file.

Qualification: Everyone is qualified, and encouraged to install and use Tripwire.

Implementation Issues: Tripwire takes some time to configure properly.

Constraints and Limitations: The information Tripwire provides is only accurate if the Tripwire configuration file and the Tripwire database file are secure. To ensure the most accurate results, backups of those files must be made, via some external media, and stored in a secure place. The database and configuration files should then be replaced with the backups prior to a Tripwire run. This is especially true if you suspect that your system has been compromised. In that event, it may also be necessary to reinstall the Tripwire binary. Complete instructions/recommendations are included in the Installation Instructions and the Release Notes.

Dependencies: None.

Installation Procedures (IP)
Tripwire 1.0.0.2 for Solaris 2.5.1
31 January 1997

Hardware and Software Requirements: Tripwire requires only that the DII COE be installed on a Hewlett Packard machine.

Installation Instructions:

1. Install the segment using ordinary segment installation procedures.
2. Detailed instructions on how to set up and configure Tripwire to run on your system are given immediately after installation in an xterm window. Instructions are also available in the ReleaseNotes. A brief outline of those instructions follows.
   a) Edit the tripwire configuration file (/h/COE/Comp/TRIP/data/TRIP.config).
   b) Create the database file.
   c) Configure Tripwire to run weekly if desired.
3. Refer to the Operator's Manual for instructions on running Tripwire.

Operator’s Manual (OM)
Tripwire 1.0.0.2 for Solaris 2.5.1
31 January 1997

Introduction: Tripwire is an integrity checker. It allows you to know if certain files you have told Tripwire to check have been changed or altered. If you check all important files on your system that do not change frequently, you will significantly improve your system security.

To run via icon: Simply double click on the Tripwire icon. You will be asked whether you want to replace the database (/h/COE/Comp/TRIP/bin/databases/TRIP.database) and configuration files with their backups. If you choose ‘y’, and xterm will appear for you to replace the files. Next, you will be asked whether you wish to run Tripwire in interactive mode. This mode allows you to update your database file for any valid changes to the files being checked. See below (Updating the Database File) for more information. When run via icon, Tripwire will send the results of the run to standard output, i.e. to the screen. This output is not saved, so if you close the xterm before you are done, you will have to run Tripwire again.

To run via crontab: Tripwire will run automatically every week early Sunday morning, if this setting was enabled at installation, either manually or by running /h/COE/Comp/TRIP/Scripts/TRIP.tripwire_weekly_config. In this case, the output will be mailed to sysadmin, and will be saved in /h/COE/Comp/TRIP/data/tripwire.results. If you only run Tripwire via crontab, you shuld ensure that the database and configuration files are secure. It is highly recommended that you run Tripwire via icon (and replace the database and configuration files) regularly, because an intruder could have found and amended the files to cover up changes to your system.

Updating the Database File: There may be valid changes to the files and/or directories Tripwire checks. In this case, it is necessary to update the database file to reflect the changes. There are two ways of doing this:
1) Run Tripwire via the Tripwire icon, and chose interactive mode. This will allow incremental updates to the database file. You will be prompted whether or not to update the entry in the form, “---> Update entry? [YN(y)ng?]”. The choices ‘y’ and ‘n’ are conventional yes and no, while ‘Y’ and ‘N’ tell tripwire yes or no for all updates. The choices ‘h’ and ‘?’ give help and descriptions of the various inode fields. You should use caution in choosing the ‘Y’ option, as that may update the database file for changes that you haven’t considered yet. It is strongly recommended that you refrain from using the ‘Y’ choice. When you are done updating the database file, DO NOT forget to update your backup copies of the database file.
2) If you have made major changes to your system, or you have updated the Tripwire configuration file (/h/COE/Comp/TRIP/data/TRIP.config), you should generate a new database file according to the original installation procedures (available in Release Notes). Be certain, however, that your system is clean BEFORE regenerating the database file, or else the corrupted files will be recognized by Tripwire as valid. Once again, do not forget to backup your database and configuration files.
3) There is a third, command-line driven option, described in the README file (in ReleaseNotes) section 3.5.2. It is complicated but feel free to use it if you so desire.

In case of Intrusion: If you know or suspect that an intruder has gained access to your system: At the minimum, replace the database and configuration files with the ones you have on your backup media. It is also recommended that you reinstall Tripwire from the original distribution, as the actual Tripwire binaries may have become corrupted. If you you reinstall Tripwire, DO NOT follow the original installation instructions and create a new database file. Instead, just copy your backups into the appropriate place, and run Tripwire normally. This should tell you of all the changes to the files you have told Tripwire to monitor.